Open Access Library Journal
2022, Volume 9, e8460
ISSN Online: 2333-9721
ISSN Print: 2333-9705

Discussion on Different Authentication Mechanisms of PKI and CPK System

Xianghao Nan

CPK Laboratory, Beijing, China
Email: nanxianghao@bochtec.com

How to cite this paper: Nan, X.H. (2022) Discussion on Different Authentication Mechanisms of PKI and CPK System. *Open Access Library Journal*, **9**: e8460.
https://doi.org/10.4236/oalib.1108460

Received: February 8, 2022
Accepted: March 7, 2022
Published: March 10, 2022

Abstract

Subject authentication is the core technology of cyber security. There are two existing technologies: one is PKI public key system based on trust logic, another is CPK public key system based on truth logic. In this paper, the different characteristics of trust-based PKI and evidence-based CPK different mechanisms were discussed from Four aspects: decentralized or centralized key generation, trust-based or evidence-based authentication logic, different usages of DSS signature protocol, and functions and performances under different mechanism. Decentralized system has too strong exclusivity, which is easy to be used by criminal groups and gangdoms. Both PKI and CPK can transform DSS signature into digital signature, but there is a serious gap in performance under different logic. Trust logic is the product of the situation that cannot prove subject authenticity. The method of certificate increases the amount of information and the burden of certificate verification.

Subject Areas

Information and Communication: Security, Privacy, and Trust

Keywords

PKI, CPK, Authentication, Trust, Evidence, Logic, Cyber

1. Introduction

Subject authentication is the core technology of cyber security, but it has been a difficult problem. Recently, the "zero trust architecture" project [1] put forward by the U.S. DoD and the federal government has once again put issue of trust on the crest of a wave. In 2005, PITAC proposed "mutual suspicion" as a security principle for the first time in its report of "Cyber Security" [2]. This is an epoch-making conclusion. This was a watershed in the development of authen-

tication theory, but after 20 years, it still remains in the age of trust logic and has not made any progress. According to the experience of U.S. military cyber warfare [3], the most effective means of network attack is to obtain login through password and take over system rights by trust transfer, thus trust transfer has become a hidden danger of security. Both the U.S. DoD and the federal government recently proposed a "zero-trust architecture" [3], saying, "Never trust, always verify", and for the first time introduced the concept of identifier to distinguish it from identity. This is a new step forward.

There are two kinds of authentication technology: one is the PKI certification system based on trust, another is the CPK authentication system based on evidence. Through these two systems, the difference between trust mechanism and zero-trust mechanism in the authentication system is studied, and the discussion is further deepened, so that our theoretical research on cyber security is on the right track. In fact, the proposal of "mutual suspicion" and "zero trust" has sounded the end of the era of trust logic, while the rise of evidence-based authentication logic is lighting the fire of the development of new logic.

2. Decentralized or Centralized Mechanisms

2.1. PKI Decentralized Mechanism

The system in which the key pair is generated by individual is called decentralized system. With the emergence of the Internet, the concept of decentralized system brought about a new problem under the new situation of public network which has broken the boundary of private network. In the past, private networks were used by the military and related government departments, but now they are used by all Internet users. At this time, asymmetric public key system appeared, which can realize the closure of arbitrary communicating two sides in public network. The National Security Agency (NSA) realized that its plans to migrate classified managing method of closed LAN security to the open Internet would not work and had to explore a new way. The reason is very simple, the technology has developed to close the two communicating sides, there is no need for classified closure. The policy of civil-military integration adopted later was a major change brought about by the emergence of new technologies. In such environment, decentralized key management is put forward by PGP, the key is generated by individuals, and the public key is published. PKI distributes public keys on the basis of decentralized PGP in the form of certificates in which the public-key and identifier is bound. The Certificate form was originated on the network of the U.S. Department of Defense. The key was generated by the Key Management Center and distributed in the form of certificates, which was called the Certificate Agency (CA). PKI borrowed the form of the certificate, and called it Certificate Authentication (CA) at first, but is changed to the Certificate Authority (CA).

The system of generating private-keys by individuals is excessively exclusive, and it is also exclusive to regulators. Such exclusivity, if used by the underworld and drug cartels, will cause great difficulties in solving the case, which is ob-

viously detrimental to safeguarding national interests. Now that the CA is effectively central, what exactly is the benefit of generating private-keys by individuals? Some people say that CA crime can be prevented, but in fact, the main security threat is not CA crime, but is the criminals' crime using the binding function of CA to commit fake certificate.

2.2. CPK Centralized Mechanism

CPK centralized mode is a traditional key management mode. Whether it can meet the needs of large-scale, individual and open network is the only criterion to measure the rationality of key management. Centralization and decentralization are just different management methods, without principle differences. PKI can also be centrally managed. China Customs introduced PKI, and creatively adopted central key distribution according to the needs of its own business. The practice proves that it is feasible to transform PKI into a centralized system, and it should be the user's right to select what kind of mechanism. But in China, because the centralized system for distributing keys did not comply with China's digital signature law, the competent department refused to approve it. A specific technical method is determined in legal form, reflecting the backwardness and confusion in the regulations and management of information security in China. European electronic signature law stipulates that as long as it is approved by both parties, the signature has legal effect. It's straightforward and consistent with the law of contract respecting users' rights.

CPK implements centralized mode, because of the solution to large scaled key management, one step of horizontal management to the whole network can be achieved with a few KB matrix space which can represent infinite public-keys, and the public matrix is published, so that anyone can calculate anyone's public-key, ensuring the personalized needs allowing to be supervised. CPK is commonly recognized as a new technology, which has been suppressed for a long time in China, which cannot but show the ignorance or other motives of the competent authorities, and further illustrate the urgency of the corresponding institutional reform with the development of new technology.

3. Trust Logic or Truth Logic

3.1. PKI Trust Logic

PKI certification system is the product of trust logic, and the proof by third party is a last resort in the case that one cannot prove his own authenticity. In the book of IATF (Information Assurance Technical Framework), the trust transfer of PKI is described as follows: If a trust relationship is established between two CAs, the employees of the two CAs have the same trust relationship. Schnaier has said that if this logic holds, it could lead to the joke that UCLA graduates can go to MIT to get their diplomas. In fact, the international standard CC described that trust transfer causes trust dilution, so the transfer should not be more than four times. The initial PKI attempts to increase the number of CA by trust

transfer to solve the problem of large-scale key management. Obviously, IATF's understanding is wrong.

We have to see that the current key management mechanism, whether centralized KDC or decentralized CA mechanism, still follows the principle of trust, and the existing trust logic based on behavior and belief logic based on model reasoning [4] are still not free from the bondage of trust relationship. This is because there is a core technology that has not been addressed. The Obama administration considered that the core technology was Identity authentication. As identity is an abstract noun and the combination of identity and ontology, identity authentication must solve the identifier authenticity and ontology authenticity as well as the oneness of identifier and ontology. Ontological features are easy to prove, such as biological characteristics, social status, etc., but ontological features are only applicable to face-to-face authentication, not remote authentication, because the oneness of identifier and ontology cannot be proved, that is, to whom this feature belongs. The only thing that can represent the subject is the identifier that the subject claims. An identifier is the name of an entity that distinguishes it from another entity, such as a phone number when making a call, a user-name when sending an email. Therefore, the core technology to prove subject authenticity is identifier authentication. If a KDC or CA center cannot prove the authenticity of the claimed identifier, it can only operate on trust.

3.2. CPK Truth Logic

CPK authentication system executes truth logic. In truth logic, identifier and identity have long been distinguished, and identity is defined as the unity of identifier and ontology. The authenticity of identity can be solved only when the authenticity of identifier is solved. In 2005, PITAC declared in its report of "Cyber Security" that "Cyber security is so complicated, there is no silver bullet". However, in 2006, CPK found a "silver bullet" and solved identifier authentication [5], because once identifier authentication was solved, other security certification become as simple as stacking wood, so the identifier authentication has become the core technology of cyber security. Truth logic is an authentication logic based on evidence, consists of evidence-showing system and evidence-verifying system, in which what evidence is shown, what evidence is verified. Without evidence there is nothing to be verified. From the perspective of theoretical research, authentication logic only stays on trust logic, the theory is unable to move forward, because the establishment of trust relationship is not the ultimate goal to be achieved by the authentication system, but is to prove the authenticity of the subject to achieve information assurance. Because the truth logic solved the problem of the authenticity of the identifier claimed by the subject, it can prove the authenticity of the key management center itself, hence the key distribution breaks away from trust logic and opens up a new key distribution method based on proof relation. In terms of CPK system, the relation between users and the KDC is a proof relation, where the authenticity of the center can be proved, and the authenticity of public matrix can also be proved, Independent of trust,

the proof system becomes more and more complete. Trust as a sociological term, plays an important role, but the authentication system is a proof system, proof needs evidence, not trust, proof has nothing to do with trust. There is no need for any additional provisions in the proof, because artificial provisions fall under the category of trust.

4. DSS Signature or Digital Signatures

4.1. PKI's DSS Signature

The digital signature standard DSS [6] is a very clever mathematical formula, in which the signer calculates a check code c with a random number and sign code s with private-key, and the verifier calculates the check code c' with the given sign code s and corresponding public-key, when $c = c'$, it proves that the private-key and public-key used are a key-pair, thus a trust relationship between the signer and verifier is established, however, it is not yet a signature, because a digital signature is a proof of the authenticity of subject and responsibility for the object, while DSS does not have the above two functions. To convert DSS into a digital signature, the PKI approach is to have the CA center provide proof of identity and public key binding, so that the DSS signature and the CA certificate are combined to form the digital signature, but this can only be set up if the CA is verified to be true.

In addition, a digital signature should have the same lifetime as the signed document, the key cannot be replaced during the validity period of the document. However, in the individualized decentralized system, the key can be changed, so the validity of the certificate is needed to be verified.

4.2. CPK's Digital Signature

CPK adopts is a modified DSS, called CPK signature protocol. The signature is the proof of the responsibility of the subject to the object, but the authenticity of the subject is proved first before proving object. Since the subject authenticity is achieved through the identifier authentication, the authenticity of the identifier claimed by the subject should be solved first. The principle to prove the authenticity of identifier is simple, first use random number k to generate check code c: $k\mathrm{G} = (\mathrm{x}, \mathrm{y}) \rightarrow c$, then use random number k and private-key sk to generate proof code s: $k^{-1}sk \bmod n = s$, its verification is to use proof code s and public-key PK to calculate the check code c': $s^{-1}PK = k\mathrm{G} \rightarrow c'$. If $c = c'$, it is proved that sk and PK are a key-pair, thus the authenticity of the key is proved. If the keys are directly generated by the identifier, a one-to-one mapping is formed between the identifier and the key, and the authenticity of the key directly proves the authenticity of the identifier. After the authenticity of the subject is proved, the proof of the object can be realized by DSS, because the DSS already includes items for identifier authentication, a signature simultaneously proves the authenticity of the subject and object, and provides proof of traceability, attribution, and responsibility, thus becoming a real digital signature protocol. The public key ma-

trix of CPK is published with the signature of key management center, so the authenticity of the subject (key management center) and the public matrix (object) can be verified by everyone, the scope and the proof relationship are clear, which is the biggest difference from CA.

5. Functions of PKI and CPK

The following takes network communication as an example to compare the functions of the authenticating mode of PKI and CPK in each link of communication. Communication events are divided into two events, sending events occur at the sending end, receiving events occur at the receiving end, sending events and receiving events constitute a virtual internet of event (IoE). In the IoE, it is up to the sender to send information, including malware like viruses, at will. But the actual control is in the hands of the receiving side, which has the right to decide whether to accept or reject, and whether to process or not. As the authentication system is the unification of the proof system and the verification system, the proof of authenticity should be provided in the sending event to ensure that the verification can be passed in the receiving event.

5.1. CPK Communication Event

The sender provides the authenticity evidence of the subject, slave, and object. For example, router IP_{Alfa} sends data to router IP_{Beta}, then IP_{Alfa} is the subject, IP_{Beta} is the slave, and data is the object.

There are two cases of sending event. One is the case where the receiver needs to separate "proof before event" and "proof after event", such as online communication with a large volume of business; the second is the case that does not need to be handled separately, such as offline communication like E-mail. Among them, proof before event is carried out before data transmission, while proof after event is carried out after data transmission. Proof of before event and after event is independent of each other.

5.1.1. CPK Sending Event

Evidence for proof before event includes proof of the authenticity of the sending address IP_{Alfa} and destination address IP_{Beta}, and proof of the authenticity of the data is provided separately: CPK executes the CPK signature protocol.

Evidence for proof before event, there are three types:

The first type: to compute the static identifier authenticity code SIC to replace the traditional "password certification", but does not prevent replication attacks:

$$k_1 \mathrm{G} = \left(x_0, y_0\right); \left(x_0 + y_0\right)^2 \bmod 2^{32} = c_1$$

$$\left(k_1^{-1} s k_{\mathrm{Alfa}}\right) \bmod n = s_1$$

$$\mathrm{SIC} = \left(s_1, c_1\right)$$

The second type: to compute the dynamic identifier authenticity code DIC to replace the traditional dynamic password. The private-key is added to time to prevent copy and DOS attacks:

$$\left(k_1^{-1}\left(sk_{\text{Alfa}}+\text{time}\right)\right)\bmod n=s_1$$

$$\text{DIC}=\left(s_1,c_1\right)$$

The third type: the subject signs to slave

$$k_1^{-1}\left(\text{IP}_{\text{Beta}}+sk_{\text{Alfa}}\right)\bmod n=s_1$$

$$\text{Sign}=\left(s_1,c_1\right)$$

Evidence for proof after event is the signature of subject to object

$$k_2\text{G}=\left(x_0,y_0\right);\ \left(x_0+y_0\right)^2\bmod 2^{32}=c_2$$

$$k_2^{-1}\left(\text{data}+sk_{\text{Alfa}}\right)\bmod n=s_2$$

$$\text{Sign}=\left(s_2,c_2\right)$$

where, k is a random number, G is the generator, sk_{Alfa} is the private key of IP_{Alfa}, c is the check code, s is the signature code, and (s, c) constitutes the signature. A signature simultaneously certifies the authenticity of subject, slave and object.

The sender can encrypt data using CPK key encryption protocol.

First computes the public-key PK_{Beta} of the receiver (IP_{Beta}):

$$\text{Hash}\left(\text{IP}_{\text{Beta}}\right)=v_i;\ \sigma\sum\text{R}_{v_i}=PK_{\text{Beta}}$$

Encrypts the data encryption key with the other party's public key PK_{Beta}

$$k\text{G}\to\text{key};\ \text{E}_{\text{key}}\left(\text{data}\right)=\text{code};\ k*PK_{\text{Beta}}=\lambda$$

Sends (code, λ) to Beta.

5.1.2. CPK Receiving Event

The receiving event mainly verifies the sender's evidence, including IP_{Alfa}, IP_{Beta} and data authenticity. The verification Implements CPK protocol and GAP one-step protocol [7].

When verifying, first calculates the signer's public-key PK_{Alfa} with the identifier:

$$\text{Hash}\left(\text{IP}_{\text{Alfa}}\right)=v_i,\ \sum\text{R}_{[v_i]}\to PK_{\text{Alfa}}$$

The verification before event is as follows:

The first type: to verify static identifier authenticity code, directly proves the authenticity of the subject:

$$s_1^{-1}PK_{\text{Alfa}}=k\text{G}\to c_1'$$

The second type: to verify dynamic identifier authenticity code: directly proves the authenticity of the subject:

$$s_1^{-1}\left(PK_{\text{Alfa}}+\text{timeG}\right)=k\text{G}\to c_1'$$

The third type: to verify the authenticity of the slave: to prove the authenticity of the subject and the slave simultaneously;

$$s_1^{-1}\left(\text{IP}_{\text{Beta}}\text{G}+PK_{\text{Alfa}}\right)=k\text{G}\to c_1'$$

The verification after event is carried out after the data is received, to prove

the authenticity of the subject and object simultaneously;

$$s_2^{-1}\left(\text{dataG}+PK_{\text{Alfa}}\right)=k\text{G}\to c_2'$$

If the data is encrypted, first decrypts data before authentication. Beta uses its own private-key to decrypt the data encryption key:

$$sk_{\text{Beta}}^{-1}*\lambda=\text{key}$$

Decrypt data with data encryption key:

$$\text{D}_{\text{key}}\left(\text{code}\right)=\text{data}$$

5.2. PKI Communication Event

5.2.1. PKI Sending Event

Evidence for proof before event:

Traditional symmetric password authentication;

Static certificate: to simulate CPK static password;

Dynamic certificate: to simulate CPK dynamic password.

Evidence for proof after event: executes the DSS signature protocol.

$$k_1\text{G}=\left(x_0,y_0\right);\ x_0 \bmod n\to c_1$$

$$k_1^{-1}\left(\text{data}+c*sk\right)\bmod n=s_1$$

The authenticity proof of public-key PK bouned to identity is provided in the form of certificate:

$$\text{Hash}\left(\text{IP}_{\text{alfa}}+PK\right)=h$$

$$k_2^{-1}\left(h+sk_{\text{CA}}\right)\bmod n=s_2;$$

$\text{sign}_1=(s_1, c_1)$ and $\text{sign}_2=(s_2, c_2)$ are combined to form a complete signature.

When encrypting, PKI first ask for the other party's public-key certificate, after verification of the certificate, the data encrypting key can be encrypted with the public-key.

5.2.2. PKI Receiving Event

Verification before event:

Password authentication: passwords can be compared but do not prove the authenticity of the subject.

Static certificates: the subject is provable, but lacks certificate authencity proof.

Dynamic certificate: the subject is provable, but lacks certificate authencity proof.

Verification after event: implements DSS protocol and TSL protocol with 6-steps 13-sentences.

First use the public key PK provided by the sender's certificate to verify the signature to the data:

$$s_1^{-1}\left(\text{data}*\text{G}+c_1*PK\right)\to c_1'$$

If $c_1=c_1'$, it is proved that the private-key sk used for signature and the pub-

lic-key PK used for verification are a pair of keys, so the data is true. But there's no proof of whose signature. Since the sender's identity and public-key are bound by the certificate, the certificate is also verified:

$$\text{Hash}\left(\text{IP}_{\text{Alfa}} + PK\right) = h$$

$$s_2^{-1}\left(h * \text{G} + c_2 * PK_{\text{CA}}\right) \to c_2';$$

If $c_2 = c_2'$, it proves that this is the signature of the sender Alfa, but the authenticity of CA has not been proved.

6. Performance of CPK and PKI

The performance comparison above communication example is summarized in the following table.

Function	Matrix	Key encryption	Length of signature	Computation of verification	subject evidence	Computation of verification
PKI	CA	1) Ask for certificate 2) Veryfy certificate, 2nG 3) Key encryption, 2nG	224B + identifier	4nG	4nB	2nG
CPK	8 × 8	Key encryption, 2nG	1n + 4B = 36B	2nG	1nB	1nG
	4 × 4	Key encryption, 2nG	10B … 20B	2nG	1nB	1nG
Performance		3 proess:1 process	7:1	4:2	4:1	2:1

Note: nG in the table represents an elliptic curve operation.

Assume that a phone number is more than 10 digits and an IP address is 8 bytes. To prove the authenticity of the phone number or IP address, the CPK authentication code is 36 bytes long, while the PKI authentication code is more than 220 bytes. In the verification operation, CPK requires two elliptic curve operations, while PKI requires six operations.

7. Summary

The difference is mainly reflected in whether the authenticity of the subject can be proved and whether the function of "proof before event" can be realized, and these are the most critical elements to achieve the goal of information assurance. For example, in communication, the authenticity of the subject can be verified before data transmission, and in transaction, the authenticity of currency can be verified before payment. PKI uses certificates to recover its subject authentication function, but the authenticity of CA still relies on trust relation and the use of certificates increases the burden of certificate verification and increases the amount of information causing a big performance difference. Especially when the system is extended, the relationship between different CAs can only be trusted.

In the field of communication and areas of the economy, 5G network, satellite network, remote control, industrial Internet, digital economy booming, the de-

mand of the subject authentication is more and more urgent. In this case, it is necessary to discuss in depth whether the authentication logic is based on trust logic or non-trust logic.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] Department of Defense (DOD) (2021) Zero Trust Reference Architecture, Version 1.0.

[2] President's Information Technology Advisory Committee (2005) Cyber Security. A Crisis of Prioritization. A Report to President.

[3] Clay, W. (2004) Information Warfare and Cyber War: Capabilities and Related Policy Issues, CRS Report for Congress.

[4] Brurros, M., Abadi, M. and Needham, R. (1990) A Logic of Authentication. *ACM SIGOPS Operating Systems Review*, **23**, 1-13. https://doi.org/10.1145/74850.74852

[5] Nan, X.H. (2006) CPK on Identifier Authentication. Publishing House of Defense Industry.

[6] National Institute of Standards and Technology, INST PUB 186, Digital Signature Standards, U.S. Department of Commerce 1994.

[7] Nan, X.H. (2020) GAP One-Step Protocol. *Communication Technology*, **53**.